JOURNAL OF ALGEBRA 23, 382–403 (1972)

Central Simple Algebras Over Totally Real Fields Which Appear in $Q[G]$*

TOSHIHIKO YAMADA

Department of Mathematics, Queen's University, Kingston, Ontario, Canada

Communicated by I. N. Herstein

Received July 26, 1971

1. INTRODUCTION

Let k be a totally real subfield of a cyclotomic extension of the rational field Q. Denote by $S_Q(k)$ the subset of the Brauer group $\mathrm{Br}(k)$ of k consisting of those algebra classes which contain a simple component of the group algebra $Q[G]$ of some finite group G. According to the Brauer–Speiser theorem, every element of $S_Q(k)$ has order at most two in $\mathrm{Br}(k)$. When k is the rational field Q, the structure of $S_Q(k)$ has been determined by Benard [1] and Fields [5]. That is, they have shown that every quaternion division algebra central over Q appears in some $Q[G]$.

Let l be an arbitrary prime number, c a positive integer and ζ_{l^c} a primitive l^c-th root of unity. In this paper, we completely determine $S_Q(k)$ when k is the maximal totally real subfield $k_{l,c} = Q(\zeta_{l^c} + \zeta_{l^c}^{-1})$ of the cyclotomic field $Q(\zeta_{l^c})$. Namely, we shall prove the following:

THEOREM. *Let A be a simple algebra central over $k_{l,c}$. Then, A appears in some $Q[G]$ (up to similarity) if and only if* (i) *A has Hasse invariant 0 or $\frac{1}{2}$ at every prime $\mathfrak{p}$ of $k_{l,c}$, and* (ii) *for any rational prime p, A has the same Hasse invariant at all the primes $\mathfrak{p}$ of $k_{l,c}$ dividing p.*

Here, we outline the proof of this Theorem. In order to prove the Theorem for $k_{l,c} = Q$ (i.e., $l^c = 3$ or 4), it was enough to consider cyclic algebras (cf. [1] and [5]). When $k_{l,c}$ is not the rational field ($l^c \geqslant 5$), we must deal with crossed products. Namely, for each rational prime p which is neither the infinite prime ∞ nor l, we construct crossed products central over $k_{l,c}$ which contain finite multiplicative groups and which are spanned by these groups with rational coefficients. It turns out that at least one of these crossed products has Hasse invariant $\frac{1}{2}$ at every prime $\mathfrak{p}$ of $k_{l,c}$ dividing p, and

* This work was done while the author was a research associate at McGill University.

possibly $\frac{1}{2}$ at $\mathfrak{l}$ of $k_{l,c}$ dividing l and at $\mathfrak{p}_\infty$ of $k_{l,c}$ dividing ∞. The construction of these crossed products and the computation of their Hasse invariants are carried out in Sections 2, 3 and 4. In Section 5, we give a cyclic algebra which appears in some $Q[G]$ and which has Hasse invariant $\frac{1}{2}$ at every infinite prime $\mathfrak{p}_\infty$ of $k_{l,c}$, and possibly $\frac{1}{2}$ at $\mathfrak{l}$ dividing l. By taking tensor products of the above algebras, we see easily that every central simple algebra over $k_{l,c}$ which satisfies the conditions (i) and (ii) of our Theorem, appears in some $Q[G]$.

Finally we remark that the statement of this Theorem is not necessarily true when k is not a maximal totally real subfield of a cyclotomic field. In fact, it will be shown that the assertion of the Theorem does not hold when k is a real quadratic field $Q(\sqrt{m})$ such that m is square free and $m \equiv 3 \pmod 4$.

Notation and Terminology. Throughout this paper, $l^c \geqslant 5$, i.e., $[k_{l,c} : Q] > 1$. Z, R and C denote respectively the ring of rational integers, the real number field and the complex number field. For a positive integer n, ζ_n is a primitive n-th root of unity. The multiplicative group of integers modulo n is denoted by $Z \bmod^\times n$, and its elements are expressed as $r \bmod^\times n$, $(r, n) = 1$. For a ring A with the identity 1, $A^\times$ is the multiplicative group consisting of those elements of A which have inverses in A. $\langle a, b, \cdots \rangle$ is the group generated by $a, b, \cdots$. Let K be a finite extension of a field k. For $a \in K$, $N(K/k, a)$ is the norm of an over k. If K is normal over k, $\mathfrak{G}(K/k)$ is the Galois group of K over k. For $\sigma \in \mathfrak{G}(K/k)$ and $x \in K$, x^σ is the image of x by σ. If K is a finite abelian extension of Q, $\mathfrak{p}$ a prime of k and $\mathfrak{P}$ a prime of K lying above $\mathfrak{p}$, then $K^\mathfrak{P}/k_\mathfrak{p}$ represents the isomorphy type of the completion of K/k for $\mathfrak{P} \mid \mathfrak{p}$. If $\mathfrak{p}$ is a finite prime, $U(k_\mathfrak{p})$ denotes the subgroup of $k_\mathfrak{p}^\times$ consisting of roots of unity whose orders are relatively prime to p, $\mathfrak{p} \mid p$. It is known that $U(k_\mathfrak{p}) = \langle \zeta_{q-1} \rangle$, where $q = N(k_\mathfrak{p}/Q_p, \mathfrak{p})$. For a central simple algebra A over k, $(A/\mathfrak{p})$ denotes its Hasse invariant at $\mathfrak{p}$. It is unique modulo Z.

2. Construction of Simple Algebras for $p \neq 2$

Throughout this section, p is an odd prime number different from l. Set $K = Q(\zeta_{l^c}, \zeta_p)$ and $k = k_{l,c} = Q(\zeta_{l^c} + \zeta_{l^c}^{-1})$. The cyclotomic field K contains the subfields $Q(\zeta_{l^c})$ and $k(\zeta_p)$ such that $Q(\zeta_{l^c}) \cdot k(\zeta_p) = K$ and $Q(\zeta_{l^c}) \cap k(\zeta_p) = k$. The Galois group $\mathfrak{G}(K/Q(\zeta_{l^c}))$ (resp. $\mathfrak{G}(K/k(\zeta_p))$ is cyclic and generated by an automorphism φ (resp. ι) of K such that

$$\varphi(\zeta_{l^c}) = \zeta_{l^c}, \qquad \varphi(\zeta_p) = \zeta_p^r \qquad (r \text{ is primitive mod } p),$$
$$\iota(\zeta_p) = \zeta_p, \qquad \iota(\zeta_{l^c}) = \zeta_{l^c}^{-1}.$$

The Galois group $\mathfrak{G} = \mathfrak{G}(K/k)$ is the direct product of $\langle\varphi\rangle$ and $\langle\iota\rangle$, i.e., $\mathfrak{G} = \langle\varphi\rangle \times \langle\iota\rangle$. Define mappings α and β from $\mathfrak{G} \times \mathfrak{G}$ into $K^\times$ by the following formulas:

$$\alpha(\varphi^\nu\iota^\mu, \varphi^{\nu'}\iota^{\mu'}) = (-\zeta_{l^e})^{\nu'\gamma}\,\zeta_{l^e}^{-\delta(p-1)/2}, \tag{1}$$

$$\beta(\varphi^\nu\iota^\mu, \varphi^{\nu'}\iota^{\mu'}) = (-\zeta_{l^e})^{\nu'\gamma}[-\zeta_{l^e}^{-(p-1)/2}]^\delta, \tag{2}$$

$$(0 \leqslant \nu, \nu' \leqslant p-2, \qquad 0 \leqslant \mu, \mu' \leqslant 1)$$

$$\gamma = \begin{cases} 0, & \mu = 0, \\ 1, & \mu = 1, \end{cases} \qquad \delta = \begin{cases} 0, & \nu + \nu' < p-1, \\ 1, & \nu + \nu' \geqslant p-1. \end{cases}$$

An easy verification shows that α and β are factor sets of K/k, i.e.,

$$\alpha(\sigma, \tau)^\rho \cdot \alpha(\rho, \sigma\tau) = \alpha(\rho, \sigma) \cdot \alpha(\rho\sigma, \tau),$$

$\beta(\sigma, \tau)^\rho \cdot \beta(\rho, \sigma\tau) = \beta(\rho, \sigma) \cdot \beta(\rho\sigma, \tau)$, $\rho, \sigma, \tau \in \mathfrak{G}$. (In order to check this, it is convenient to refer to Zassenhaus [12, III, §8].) Consider the following crossed products $A = A(l^e, p)$ and $B = B(l^e, p)$ of K/k with its Galois group $\mathfrak{G}$, and having the factor sets α and β respectively:

$$A = (\alpha, K/k) = \sum_{\sigma\in\mathfrak{G}} Ku_\sigma \qquad \text{(direct sum)},$$

$$u_\sigma x = x^\sigma u_\sigma, \qquad u_\sigma u_\tau = \alpha(\sigma, \tau)\, u_{\sigma\tau} \qquad (x \in K; \quad \sigma, \tau \in \mathfrak{G}),$$

$$B = (\beta, K/k) = \sum_{\sigma\in\mathfrak{G}} Kv_\sigma \qquad \text{(direct sum)},$$

$$v_\sigma x = x^\sigma v_\sigma, \qquad v_\sigma v_\tau = \beta(\sigma, \tau)\, v_{\sigma\tau}.$$

From the definition of the factor sets α and β, it follows easily that

$$u_\iota u_\varphi = -\zeta_{l^e} u_\varphi u_\iota, \qquad u_\varphi^{p-1} = \zeta_{l^e}^{-(p-1)/2}, \qquad u_\iota^2 = 1, \tag{3}$$

$$v_\iota v_\varphi = -\zeta_{l^e} v_\varphi v_\iota, \qquad v_\varphi^{p-1} = -\zeta_{l^e}^{-(p-1)/2}, \qquad v_\iota^2 = 1. \tag{4}$$

If l is an odd prime number, the elements -1, ζ_{l^e}, ζ_p, u_φ and u_ι generate a finite subgroup $G = G(l^e, p)$ of the multiplicative group $A(l^e, p)^\times$, i.e., $G = \langle -1, \zeta_{l^e}, \zeta_p, u_\varphi, u_\iota\rangle$. In fact, G contains the normal cyclic subgroup $F_1 = \langle -1, \zeta_{l^e}, \zeta_p\rangle$ of order $2pl^e$ and G/F_1 is isomorphic to $\mathfrak{G}(Q(\zeta_{l^e}, \zeta_p)/k_{l,e})$. That is, G is an extension of F_1 by an abelian group of order $2(p-1)$, having the factor set α defined by (1). The crossed product $A = A(l^e, p)$ is spanned by G with rational coefficients, i.e., $A = \{\sum_{g\in G} a_g g;\ a_g \in Q\}$. So, A is isomorphic to a simple component of the group algebra $Q[G]$. Similarly, the elements -1, ζ_{l^e}, ζ_p, v_φ and v_ι generate a finite subgroup

$H = H(l^c, p)$ of $B(l^c, p)^\times$. H is an extension of the normal cyclic subgroup $F_2 = \langle -1, \zeta_{l^c}, \zeta_p \rangle$ by an abelian group isomorphic to $\mathfrak{G}(K/k)$, having the factor set β. $B = B(l^c, p)$ is isomorphic to a simple component of $Q[H]$. If $l = 2$, then $G(2^c, p) = \langle \zeta_{2^c}, \zeta_p, u_\varphi, u_\iota \rangle$ is a finite subgroup of $A(2^c, p)^\times$. $G(2^c, p)$ is an extension of the normal subgroup $I_1 = \langle \zeta_{2^c}, \zeta_p \rangle$ of order $2^c p$ by an abelian group isomorphic to $\mathfrak{G}(Q(\zeta_{2^c}, \zeta_p)/k_{2,c})$, having the factor set α. The crossed product $A(2^c, p)$ is spanned by $G(2^c, p)$ with rational coefficients, and so it is isomorphic to a simple component of the group algebra $Q[G(2^c, p)]$. By the same reason, $H(2^c, p) = \langle \zeta_{2^c}, \zeta_p, v_\varphi, v_\iota \rangle$ is a finite subgroup of $B(2^c, p)^\times$, and the crossed product $B(2^c, p)$ is isomorphic to a simple component of $Q[H(2^c, p)]$. Thus we have shown that for every l and c and for every p ($\neq 2, l$), the simple algebras $A(l^c, p)$ and $B(l^c, p)$ central over $k_{l,c}$ appear in some $Q[G]$.

Now we are going to calculate the Hasse invariants of the crossed products $A = A(l^c, p)$ and $B = B(l^c, p)$. If $\mathfrak{q}$ is a prime ideal of $k_{l,c}$ which divide neither l nor p, both A and B have Hasse invariant zero at $\mathfrak{q}$, because $\mathfrak{q}$ is not ramified in $Q(\zeta_{l^c}, \zeta_p)/k_{l,c}$ and the factor sets α and β consist of roots of unity. So, we have

$$(A(l^c, p)/\mathfrak{q}) = (B(l^c, p)/\mathfrak{q}) = 0, \qquad \text{for} \quad \mathfrak{q} \nmid l, p. \tag{5}$$

The elements $u_\varphi{}^\nu u_\iota{}^\mu$ ($\nu = 0, 1, \ldots, p-2$; $\mu = 0, 1$) are linearly independent over K (cf. van der Waerden [9, p. 211]). The elements $\{(1 - \zeta_{l^c}) u_\varphi\}^\nu u_\iota{}^\mu$ ($\nu = 0, 1, \ldots, p-2$; $\mu = 0, 1$) are also linearly independent over K. From (3), it follows that

$$\begin{aligned} u_\iota\{(1 - \zeta_{l^c}) u_\varphi\} &= (1 - \zeta_{l^c}^{-1}) u_\iota u_\varphi = (1 - \zeta_{l^c}^{-1})(-\zeta_{l^c}) u_\varphi u_\iota , \\ &= \{(1 - \zeta_{l^c}) u_\varphi\} u_\iota . \end{aligned}$$

Each element of $Q(\zeta_{l^c})$ (resp. $k(\zeta_p)$) commutes with $(1 - \zeta_{l^c}) u_\varphi$ (resp. u_ι). Consequently, we have

$$\begin{aligned} A &= \sum_{\mu=0}^{1} \sum_{\nu=0}^{p-2} K u_{\varphi^\nu \iota^\mu} = \sum_\mu \sum_\nu Q(\zeta_{l^c}) \cdot k(\zeta_p)\{(1 - \zeta_{l^c}) u_\varphi\}^\nu u_\iota{}^\mu, \\ &= \left[\sum_{\nu=0}^{p-2} k(\zeta_p)\{(1 - \zeta_{l^c}) u_\varphi\}^\nu\right] \cdot \left[\sum_{\mu=0}^{1} Q(\zeta_{l^c}) u_\iota{}^\mu\right], \\ &\cong (\{(1 - \zeta_{l^c}) u_\varphi\}^{p-1}, k(\zeta_p)/k, \varphi) \otimes_k (u_\iota{}^2, Q(\zeta_{l^c})/k, \iota), \\ &= ((1 - \zeta_{l^c})^{p-1} u_\varphi^{p-1}, k(\zeta_p)/k, \varphi) \otimes_k (1, Q(\zeta_{l^c})/k, \iota), \\ &\sim (\{(1 - \zeta_{l^c})^2 \zeta_{l^c}^{-1}\}^{(p-1)/2}, k(\zeta_p)/k, \varphi). \end{aligned}$$

Concerning the above isomorphism, we note that the dimension of A over k is equal to the dimension of the tensor product

$$(\{(1-\zeta_{l^e})u_\varphi\}^{p-1}, k(\zeta_p)/k, \varphi) \otimes_k (u_\iota^2, Q(\zeta_{l^e})/k, \iota).$$

By the same argument, we have

$$\begin{aligned} B &= \sum_{\mu=0}^{1}\sum_{\nu=0}^{p-2} Kv_{\varphi^\nu\iota^\mu} = \sum_{\mu}\sum_{\nu} Q(\zeta_{l^e})\cdot k(\zeta_p)\{(1-\zeta_{l^e})v_\varphi\}^\nu v_\iota^\mu, \\ &\cong (\{(1-\zeta_{l^e})v_\varphi\}^{p-1}, k(\zeta_p)/k, \varphi) \otimes_k (v_\iota^2, Q(\zeta_{l^e})/k, \iota), \\ &\sim (-\{(1-\zeta_{l^e})^2\zeta_{l^e}^{-1}\}^{(p-1)/2}, k(\zeta_p)/k, \varphi), \\ &\sim A \otimes_k (-1, k(\zeta_p)/k, \varphi). \end{aligned}$$

Here $(1-\zeta_{l^e})^2\zeta_{l^e}^{-1}$ is an element of $k = k_{l,e}$ and the principal ideal $\mathfrak{l} = ((1-\zeta_{l^e})^2\zeta_{l^e}^{-1})$ is the only prime ideal of the integer ring of k dividing l, i.e.,

$$(l) = \mathfrak{l}^{l^{e-1}(l-1)/2} \quad \text{for} \quad l \neq 2, \qquad (2) = \mathfrak{l}^{2^{e-2}} \quad \text{for} \quad l = 2.$$

So, $\pi = (1-\zeta_{l^e})^2\zeta_{l^e}^{-1}$ is a prime element of the local field $k_\mathfrak{l}$. Let f_1 be the smallest positive integer such that $l^{f_1} \equiv 1 \pmod p$ and set $g_1 = (p-1)/f_1$. Then the extension $k(\zeta_p)^\mathfrak{l}/k_\mathfrak{l}$ is nonramified of degree f_1 and

$$\begin{aligned} A \otimes_k k_\mathfrak{l} &\sim (\pi^{(p-1)/2}, k(\zeta_p)^\mathfrak{l}/k_\mathfrak{l}, \varphi^{g_1}), \\ B \otimes_k k_\mathfrak{l} &\sim (A \otimes_k k_\mathfrak{l}) \otimes_{k_\mathfrak{l}} (-1, k(\zeta_p)^\mathfrak{l}/k^\mathfrak{l}, \varphi^{g_1}), \\ &\sim A \otimes_k k_\mathfrak{l}. \end{aligned}$$

Here we note that $(-1, k(\zeta_p)^\mathfrak{l}/k_\mathfrak{l}, \varphi^{g_1}) \sim 1$, because $k(\zeta_p)^\mathfrak{l}/k_\mathfrak{l}$ is nonramified and -1 is a unit. From the definition of Hasse invariant, it follows that the Hasse invariants of the crossed products $A = A(l^e, p)$ and $B = B(l^e, p)$ at $\mathfrak{l}$ are equal to

$$\frac{(p-1)/2}{f_1} = \frac{f_1 g_1}{2f_1} = \frac{g_1}{2}.$$

An easy verification shows that if the Legendre symbol (l/p) is equal to 1, then g_1 is an even number, and if $(l/p) = -1$, then g_1 is odd. Hence, for the prime ideal $\mathfrak{l}(\mathfrak{l} \mid l)$ of $k_{l,e}$, we have

$$\left(\frac{A(l^e, p)}{\mathfrak{l}}\right) = \left(\frac{B(l^e, p)}{\mathfrak{l}}\right) = \begin{cases} 0, & \text{if} \quad (l/p) = 1, \\ \frac{1}{2}, & \text{if} \quad (l/p) = -1. \end{cases} \tag{6}$$

For the case $l = 2$, this equation can be written as follows:

$$\left(\frac{A(2^e, p)}{\mathfrak{l}}\right) = \left(\frac{B(2^e, p)}{\mathfrak{l}}\right) = \begin{cases} 0, & \text{if} \quad p \equiv \pm 1 \pmod 8, \\ \frac{1}{2}, & \text{if} \quad p \equiv \pm 5 \pmod 8, \end{cases} \tag{7}$$

because we have the formula $(2/p) = (-1)^{(p^2-1)/8}$ (cf. [7, p. 92]).

Let $\mathfrak{p}_\infty$ be an infinite prime of $k = k_{l,c}$. We see easily that

$$\pi = (1 - \zeta_{l^c})^2 \zeta_{l^c}^{-1} = \zeta_{l^c} + \zeta_{l^c}^{-1} - 2 < 0,$$

$$A(l^c, p) \otimes_k k_{\mathfrak{p}_\infty} \sim (\pi^{(p-1)/2}, k(\zeta_p)^{\mathfrak{p}_\infty}/k_{\mathfrak{p}_\infty}, \varphi^{(p-1)/2}),$$

$$\cong (\pi^{(p-1)/2}, C/R, \rho), \quad (\rho(\sqrt{-1}) = -\sqrt{-1}),$$

$$B(l^c, p) \otimes_k k_{\mathfrak{p}_\infty} \sim (-\pi^{(p-1)/2}, C/R, \rho),$$

$$\pi^{(p-1)/2} > 0, \quad \text{if} \quad p \equiv 1 \pmod 4,$$

$$\pi^{(p-1)/2} < 0, \quad \text{if} \quad p \equiv -1 \pmod 4.$$

Hence, for any infinite prime $\mathfrak{p}_\infty$ of $k_{l,c}$, we have

$$\left(\frac{A(l^c, p)}{\mathfrak{p}_\infty}\right) = \begin{cases} 0, & \text{if} \quad p \equiv 1 \pmod 4, \\ \frac{1}{2}, & \text{if} \quad p \equiv -1 \pmod 4, \end{cases} \tag{8}$$

$$\left(\frac{B(l^c, p)}{\mathfrak{p}_\infty}\right) = \begin{cases} \frac{1}{2}, & \text{if} \quad p \equiv 1 \pmod 4, \\ 0, & \text{if} \quad p \equiv -1 \pmod 4. \end{cases} \tag{9}$$

The computation of the Hasse invariants of A and B at $\mathfrak{p}$ of k dividing p, is rather complicated, so we will carry this out in the next section.

3. The Hasse Invariants at $\mathfrak{p}$

Throughout this section, $\mathfrak{p}$ denotes a prime ideal of $k = k_{l,c}$ dividing p, f the smallest positive integer such that

$$p^f \equiv 1 \pmod{l^c}. \tag{10}$$

Set

$$g'f = (l-1)\, l^{c-1} = \varphi(l^c), \quad \text{for} \quad l \neq 2, \tag{11}$$

$$g'f = 2^{c-1} = \varphi(2^c), \quad \text{for} \quad l = 2. \tag{12}$$

For simplicity, we write $A(l^c, p)_\mathfrak{p} = A(l^c, p) \otimes_k k_\mathfrak{p}$ and $B(l^c, p)_\mathfrak{p} = B(l^c, p) \otimes_k k_\mathfrak{p}$. We use the same notation as in Section 2.

Lemma 1. *For an integer n such that $0 < n < l^c$, write $n = vl^s$, $(v, l) = 1$. Then l^{c-s} divides the binomial coefficient $\binom{l^c}{n}$.*

Proof. Set $N = \binom{l^c}{n}$. Then, $N = (l^c/n)t$, where $t = \binom{l^c-1}{n-1}$, and so, $nN = l^c t$. From this, the assertion follows immediately.

Lemma 2. *Suppose that $l \neq 2$. If r is a primitive root* mod l^c, i.e., *$\langle r \bmod^\times l^c \rangle = Z \bmod^\times l^c$, then r is also a primitive root* mod l.

Proof. If $r^t \equiv 1 \pmod{l}$ for some $t \in Z$, write $r^t = 1 + lw$, $w \in Z$. Then, $r^{tl^{c-1}} = (1 + lw)^{l^{c-1}} \equiv 1 \pmod{l^c}$, as easily follows from Lemma 1. Hence, $(l-1)\,l^{c-1}$ divides tl^{c-1}, and so $l - 1$ divides t.

LEMMA 3. *Suppose that $l \neq 2$. If f is odd, then $\mathfrak{p}$ splits into two primes in $Q(\zeta_{l^c})$. If f is even, then $\mathfrak{p}$ is inertial in $Q(\zeta_{l^c})$. g' is odd if and only if the Legendre symbol (p/l) is equal to -1.*

Proof. We identify the Galois group $\mathfrak{G} = \mathfrak{G}(Q(\zeta_{l^c})/Q)$ with the multiplicative group $Z \bmod^{\times} l^c$. The decomposition group $\mathfrak{T}$ of p in $\mathfrak{G}$ is the cyclic group $\langle p \bmod^{\times} l^c \rangle$. Since $\mathfrak{G}(Q(\zeta_{l^c})/k_{l,c}) = \langle -1 \bmod^{\times} l^c \rangle$, $\mathfrak{p}$ is inertial in $Q(\zeta_{l^c})/k_{l,c}$ if and only if $-1 \bmod^{\times} l^c \in \langle p \bmod^{\times} l^c \rangle$. As $Z \bmod^{\times} l^c$ is cyclic of order $(l-1)\,l^{c-1}$, $-1 \bmod^{\times} l^c$ is the only element of order 2. Recall that f is the order of the cyclic subgroup $\langle p \bmod^{\times} l^c \rangle$ of $Z \bmod^{\times} l^c$. Hence f is even, if and only if $-1 \bmod^{\times} l^c \in \langle p \bmod^{\times} l^c \rangle$. As to the last assertion of Lemma 3, we note that g' is odd if and only if t is odd, where $p \equiv r^t \pmod{l^c}$ and r is a primitive root mod l^c. From Lemma 2, it follows readily that t is odd if and only if $(p/l) = -1$.

LEMMA 4. *Suppose that $l = 2$. If $p \not\equiv -1 \pmod{2^c}$, then $\mathfrak{p}$ splits into two primes in $Q(\zeta_{2^c})$, and if $p \equiv -1 \pmod{2^c}$, then $\mathfrak{p}$ is inertial in $Q(\zeta_{l^c})$. Let g be the number of the prime ideals of $k_{2,c}$ which divide p. If $p \equiv \pm 1 \pmod 8$, then g is even, and if $p \equiv \pm 5 \pmod 8$, then $g = 1$, i.e., p is inertial in $k_{l,c}/Q$ $(c \geqslant 3)$. If $p \not\equiv \pm 1 \pmod{2^c}$, then $p^f \not\equiv 1 \pmod{2^{c+1}}$.*

Proof. We know that $Z \bmod^{\times} 2^c = \{(-1)^i \cdot 5^j \bmod^{\times} 2^c;\ i = 0, 1,\ j = 0, 1, \ldots, 2^{c-2} - 1\}$ (cf. [7, p. 78]). An easy verification shows that $-1 \bmod^{\times} 2^c \in \langle (-1)^i \cdot 5^j \bmod^{\times} 2^c \rangle$ if and only if $i = 1$, $j = 0$. Since $\mathfrak{G}(Q(\zeta_{2^c})/Q) = Z \bmod^{\times} 2^c$ and $\mathfrak{G}(Q(\zeta_{2^c})/k_{2,c}) = \langle -1 \bmod^{\times} 2^c \rangle$, $\mathfrak{p}(\mathfrak{p} \mid p)$ is inertial in $Q(\zeta_{2^c})/k_{2,c}$ if and only if $-1 \bmod^{\times} 2^c \in \langle p \bmod^{\times} 2^c \rangle$, i.e., if and only if $p \equiv -1 \pmod{2^c}$. We note that $(-1)^i \cdot 5^j \equiv \pm 5 \pmod 8$ if and only if j is odd. In this case, the cyclic group $\langle (-1)^i \cdot 5^j \bmod^{\times} 2^c \rangle$ has order 2^{c-2}, and $-1 \bmod^{\times} 2^c \notin \langle (-1)^i \cdot 5^j \bmod^{\times} 2^c \rangle$. From this, it is easily verified that if $p \equiv \pm 5 \pmod 8$, then p is inertial in $k_{2,c}/Q$, i.e., $g = 1$. If $p \equiv -1 \pmod{2^c}$, then $g = 2^{c-2}$ and this is even. If $p \not\equiv -1 \pmod{2^c}$ and $p \equiv (-1)^i \cdot 5^j \equiv \pm 1 \pmod 8$, then j is even and so the order of $\langle p \bmod^{\times} 2^c \rangle$ is at most 2^{c-3}. Consequently, 4 divides g' and 2 divides g. If $p \equiv (-1)^i \cdot 5^j \not\equiv \pm 1 \pmod{2^c}$, $j = 2^\lambda v$, $(2, v) = 1$, then $0 \leqslant \lambda < c - 2$ and the order f of $\langle p \bmod^{\times} 2^c \rangle$ is equal to $2^{c-2-\lambda} (\geqslant 2)$. Write $p = (-1)^i \cdot 5^j + s2^c$, $s \in Z$. By Lemma 1, it is easily verified that

$$p^f = ((-1)^i \cdot 5^j + s2^c)^{2^{c-2-\lambda}} \equiv 5^{2^{c-2}v} \not\equiv 1 \pmod{2^{c+1}}.$$

LEMMA 5. *If $\mathfrak{P}$ is any prime ideal of $Q(\zeta_{l^c})$ dividing $\mathfrak{p}$, then $\mathfrak{P}$ is totally ramified in $Q(\zeta_{l^c}, \zeta_p)/Q(\zeta_{l^c})$. $\mathfrak{p}$ is also totally ramified in $k_{l,c}(\zeta_p)/k_{l,c}$.*

Proof. This lemma is obvious.

LEMMA 6. *Let y be a rational prime number, and $L_\mathfrak{y}$ and $F_\mathfrak{y}$ be finite extension fields of the y-adic field Q_y with the maximal ideals $\mathfrak{Y}$ and $\mathfrak{y}$ respectively such that $L_\mathfrak{y} \supset F_\mathfrak{y}$. Set $N(L_\mathfrak{y}/Q_y, \mathfrak{Y}) = y^h$, $N(F_\mathfrak{y}/Q_y, \mathfrak{y}) = y^d$, $U(L_\mathfrak{y}) = \langle \zeta_{y^h-1} \rangle$ and $U(F_\mathfrak{y}) = \langle \zeta_{y^d-1} \rangle$. Then, an element x of $U(F_\mathfrak{y})$ belongs to $N(L_\mathfrak{y}/F_\mathfrak{y}, L_\mathfrak{y}^\times)$, if and only if x belongs to $N(L_\mathfrak{y}/F_\mathfrak{y}, U(L_\mathfrak{y}))$.*

Proof. Let e be the ramification index of $\mathfrak{Y}$ over $\mathfrak{y}$. Then, $E = F_\mathfrak{y}(\zeta_{y^h-1})$ is the maximal unramified extension of $F_\mathfrak{y}$ in $L_\mathfrak{y}$, and $[L_\mathfrak{y} : E] = e$. Since $N(E/F_\mathfrak{y}, \zeta_{y^h-1})$ is a primitive $(y^d - 1)$-th root of unity, we can assume that $\zeta_{y^d-1} = N(E/F_\mathfrak{y}, \zeta_{y^h-1})$. It is well-known that every element z of $L_\mathfrak{y}^\times$ has a unique expression

$$z = \pi^s \zeta_{y^h-1}^r \rho; \qquad s \in Z, \quad r \bmod y^h - 1, \quad \rho\text{: principal unit of } L_\mathfrak{y},$$

where π is a prime element of $L_\mathfrak{y}$. Hence we have

$$N(L_\mathfrak{y}^\times) = \{N(\pi)^s \zeta_{y^d-1}^{er} N(\rho);\ s \in Z,\ r \bmod y^h - 1,\ \rho\text{: principal unit of } L_\mathfrak{y}\},$$

where N denotes the norm of $L_\mathfrak{y}$ over $F_\mathfrak{y}$. We see that $N(\pi)^s \zeta_{y^d-1}^{er} N(\rho)$ is a unit of $F_\mathfrak{y}$ if and only if $s = 0$, and that $N(\rho)$ is a principal unit of $F_\mathfrak{y}$. From these facts, the assertion of Lemma 6 easily follows.

Now we proceed to calculate the Hasse invariants of $A(l^c, p)$ and $B(l^c, p)$ at $\mathfrak{p}$. Assume first that $\mathfrak{p}$ *splits into two primes in* $Q(\zeta_{l^c})/k_{l,c}$. Then we have

$$\begin{aligned}
\mathfrak{G}(K^\mathfrak{p}/k_\mathfrak{p}) &= \mathfrak{G}(K^\mathfrak{p}/Q(\zeta_{l^c})^\mathfrak{p}) = \mathfrak{G}(K/Q(\zeta_{l^c})), \\
A(l^c, p)_\mathfrak{p} &= A(l^c, p) \otimes_k k_\mathfrak{p} \sim \sum_{\nu=0}^{p-2} K^\mathfrak{p} u_\varphi^\nu, \\
&= (u_\varphi^{p-1}, K^\mathfrak{p}/k_\mathfrak{p}, \varphi), \\
&= (\zeta_{l^c}^{-(p-1)/2}, K^\mathfrak{p}/k_\mathfrak{p}, \varphi), \qquad (13) \\
B(l^c, p)_\mathfrak{p} &= B(l^c, p) \otimes_k k_\mathfrak{p} \sim \sum_{\nu=0}^{p-2} K^\mathfrak{p} v_\varphi^\nu, \\
&= (-\zeta_{l^c}^{-(p-1)/2}, K^\mathfrak{p}/k_\mathfrak{p}, \varphi), \\
&\sim (-1, K^\mathfrak{p}/k_\mathfrak{p}, \varphi) \otimes_{k_\mathfrak{p}} A(l^c, p)_\mathfrak{p}, \qquad (14)
\end{aligned}$$

where $K = Q(\zeta_{l^c}, \zeta_p)$, $k = k_{l,c}$, u_φ^{p-1} and v_φ^{p-1} are given by (3) and (4). Denote by $U(K^\mathfrak{p})$ the set of roots of unity contained in $K^\mathfrak{p}$, whose orders are

relatively prime to p. Then $U(K^{\mathfrak{p}})$ is the cyclic group generated by a primitive $(p^f - 1)$-th root of unity ζ_{p^f-1}. Since $K^{\mathfrak{p}}/k_{\mathfrak{p}}$ is totally ramified of degree $p - 1$, the image $N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}}))$ of $U(K^{\mathfrak{p}})$ by the norm of $K^{\mathfrak{p}}$ over $k_{\mathfrak{p}}$ is $\langle \zeta_{p^f-1}^{p-1} \rangle$. We summarize

$$U(K^{\mathfrak{p}}) = \langle \zeta_{p^f-1} \rangle, \qquad N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}})) = \langle \zeta_{p^f-1}^{p-1} \rangle. \tag{15}$$

Suppose that $l \neq 2$. Then we see easily that $\zeta_{l^c}^{-(p-1)/2} \in N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}}))$, because $p^f - 1 \equiv 0 \ (l^c)$ and the l part of $p - 1$ is equal to that of $(p - 1)/2$. Hence $A(l^c, p)_{\mathfrak{p}} \sim 1$, and so, by (14), $B(l^c, p)_{\mathfrak{p}} \sim (-1, K^{\mathfrak{p}}/k_{\mathfrak{p}}, \varphi)$. By Lemma 3, f is an odd number. Therefore,

$$(p^f - 1)/(p - 1) = p^{f-1} + p^{f-2} + \cdots + p + 1 \equiv f \equiv 1 \pmod 2,$$

because p is odd. Since $N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}})) = \langle \zeta_{p^f-1}^{p-1} \rangle$ and $\zeta_{p^f-1}^{p-1}$ is a primitive $(p^f - 1)/(p - 1)$-th root of unity, we conclude that $-1 \notin N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}}))$. By Lemma 6, $-1 \notin N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, (K^{\mathfrak{p}})^{\times})$. Consequently, the Hasse invariant of $B(l^c, p)_{\mathfrak{p}}$ is equal to $\frac{1}{2}$. Thus we have proved

$$[A(l^c, p)/\mathfrak{p}] = 0, \qquad [B(l^c, p)/\mathfrak{p}] = \tfrac{1}{2}, \tag{16}$$

if $l \neq 2$ and $\mathfrak{p}$ splits into two primes in $Q(\zeta_{l^c})$.

Suppose next that $l = 2$. Then, by Lemma 4, $p \not\equiv -1 \pmod{2^c}$. First we assume that $p \not\equiv \pm 1 \pmod{2^c}$. Then, $p - 1 = 2^a \cdot t$, $(2, t) = 1$, $1 \leqslant a < c$. By the last assertion of Lemma 4, the 2-Sylow subgroup of the cyclic group $\langle \zeta_{p^f-1} \rangle$ is generated by a primitive 2^c-th root of unity ζ_{2^c}. Hence, the 2-Sylow subgroup of $N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}})) = \langle \zeta_{p^f-1}^{p-1} \rangle$, is generated by $\zeta_{2^c}^{p-1}$, which is a primitive 2^{c-a}-th root of unity. Since both $\zeta_{2^c}^{(p-1)/2}$ and $-\zeta_{2^c}^{(p-1)/2}$ are 2^{c-a+1}-th root of unity, we conclude that neither $\zeta_{2^c}^{(p-1)/2}$ nor $-\zeta_{2^c}^{(p-1)/2}$ belongs to $N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}}))$, and so by Lemma 6, $\zeta_{2^c}^{(p-1)/2}, -\zeta_{2^c}^{(p-1)/2} \notin N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, (K^{\mathfrak{p}})^{\times})$. From (13) and (14), it follows that the Hasse invariants of $A(2^c, p)_{\mathfrak{p}}$ and $B(2^c, p)_{\mathfrak{p}}$ are equal to $\frac{1}{2}$. Summarizing,

$$[A(2^c, p)/\mathfrak{p}] = [B(2^c, p)/\mathfrak{p}] = \tfrac{1}{2}, \qquad \text{for} \quad p \not\equiv \pm 1 \pmod{2^c}. \tag{17}$$

Assume next that $p \equiv 1 \pmod{2^c}$, and set $p - 1 = 2^a \cdot t$, $(2, t) = 1$, $c \leqslant a$. Then, $p^f - 1 = p - 1$, i.e., $f = 1$, and so $N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}})) = \langle \zeta_{p-1}^{p-1} \rangle = \langle 1 \rangle$. If $a = c$, then $\zeta_{2^c}^{-(p-1)/2} = -1 \notin N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}}))$. If $a > c$, then $\zeta_{2^c}^{-(p-1)/2} = 1 \in N(K^{\mathfrak{p}}/k_{\mathfrak{p}}, U(K^{\mathfrak{p}}))$. Consequently, from (13) and (14), we conclude

$$[A(2^c, p)/\mathfrak{p}] = \tfrac{1}{2}, [B(2^c, p)/\mathfrak{p}] = 0, \qquad \text{if} \quad p \equiv 1 \pmod{2^c} \quad \text{and} \quad p \not\equiv 1 \pmod{2^{c+1}}, \tag{18}$$

$$[A(2^c, p)/\mathfrak{p}] = 0, \qquad [B(2^c, p)/\mathfrak{p}] = \tfrac{1}{2}, \qquad \text{if} \quad p \equiv 1 \pmod{2^{c+1}}. \tag{19}$$

Thus, for every l, we have calculated the Hasse invariants of $A(l^c, p)$ and $B(l^c, p)$ at $\mathfrak{p}$, provided that $\mathfrak{p}$ splits into two primes in $Q(\zeta_{l^c})/k_{l,c}$.

Now we assume that $\mathfrak{p}$ *is inertial in* $Q(\zeta_{l^c})/k_{l,c}$. Then we have

$$\mathfrak{G}(K^{\mathfrak{p}}/k_{\mathfrak{p}}) = \mathfrak{G}(K/k),$$

$$A(l^c, p)_{\mathfrak{p}} \sim \sum_{\nu=0}^{p-2} \sum_{\mu=0}^{1} K^{\mathfrak{p}} u_{\varphi^{\nu}\iota^{\mu}}, \tag{20}$$

$$B(l^c, p)_{\mathfrak{p}} \sim \sum_{\nu=0}^{p-2} \sum_{\mu=0}^{1} K^{\mathfrak{p}} v_{\varphi^{\nu}\iota^{\mu}}. \tag{21}$$

Suppose that $l \neq 2$. Set $q = N(k_{\mathfrak{p}}/Q_p, \mathfrak{p})$. Then $q = p^{f/2}$ and $U(K^{\mathfrak{p}}) = \langle \zeta_{p^f-1} \rangle = \langle \zeta_{q^2-1} \rangle$. Since $Z \bmod^{\times} l^c$ is cyclic, $q \bmod^{\times} l^c$ is the only element of order 2 in $Z \bmod^{\times} l^c$, and so $q \equiv -1 \pmod{l^c}$. Consequently, $q - 1 \equiv -2 \pmod{l^c}$. Let z be an integer such that $2z \equiv 1 \pmod{l^c}$. Then $(q-1)z \equiv -1 \pmod{l^c}$. Set $q^2 - 1 = 2^v \cdot h$, $(2, h) = 1$ and $q - 1 = 2^s \cdot h'$, $(2, h') = 1$. Then, $1 \leqslant s < v$, and so a primitive 2^{s+1}-th root of unity $\zeta_{2^{s+1}}$ belongs to $U(K^{\mathfrak{p}})$. Set $\gamma = \zeta_{l^c}^{z}\zeta_{2^{s+1}}$. Then, $\gamma \in U(K^{\mathfrak{p}})$, and $\gamma^{q-1} = \zeta_{l^c}^{z(q-1)}\zeta_{2^{s+1}}^{q-1} = -\zeta_{l^c}^{-1}$. When we regard the automorphism ι of K/k as that of $K^{\mathfrak{p}}/k_{\mathfrak{p}}$, ι is the Frobenius automorphism of $K^{\mathfrak{p}}/k_{\mathfrak{p}}$. Hence, $(\zeta_{q^2-1})^{\iota} = \zeta_{q^2-1}^{q}$, and so $\gamma^{\iota} = \gamma^{q}$. Consequently, by (3) and (4), we have

$$u_{\varphi}u_{\iota} = -\zeta_{l^c}^{-1}u_{\iota}u_{\varphi} = \gamma^{q-1}u_{\iota}u_{\varphi},$$

$$(\gamma u_{\varphi})\, u_{\iota} = \gamma^{q}u_{\iota}u_{\varphi} = u_{\iota}(\gamma u_{\varphi}),$$

$$v_{\varphi}v_{\iota} = \gamma^{q-1}v_{\iota}v_{\varphi}, \qquad (\gamma v_{\varphi})\, v_{\iota} = v_{\iota}(\gamma v_{\varphi}).$$

Each element of $Q(\zeta_{l^c})^{\mathfrak{p}}$ commutes with γu_{φ}, and each element of $k(\zeta_p)^{\mathfrak{p}}$ commutes with u_{ι}. Therefore, we have

$$\begin{aligned}
A(l^c, p)_{\mathfrak{p}} &\sim \sum_{\nu=0}^{p-2} \sum_{\mu=0}^{1} K^{\mathfrak{p}} u_{\varphi^{\nu}\iota^{\mu}}, \\
&= \sum_{\nu} \sum_{\mu} Q(\zeta_{l^c})^{\mathfrak{p}} \cdot k(\zeta_p)^{\mathfrak{p}}(\gamma u_{\varphi})^{\nu}\, u_{\iota}{}^{\mu}, \\
&= \Big[\sum_{\nu} k(\zeta_p)^{\mathfrak{p}}(\gamma u_{\varphi})^{\nu}\Big] \cdot \Big[\sum_{\mu} Q(\zeta_{l^c})^{\mathfrak{p}}\, u_{\iota}{}^{\mu}\Big], \\
&\cong ((\gamma u_{\varphi})^{p-1},\ k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}},\ \varphi) \otimes_{k_{\mathfrak{p}}} (u_{\iota}{}^2,\ Q(\zeta_{l^c})^{\mathfrak{p}}/k_{\mathfrak{p}},\ \iota), \\
&= (\zeta_{2^{s+1}}^{p-1},\ k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}},\ \varphi),
\end{aligned}$$

where, by (3), $u_{\iota}{}^2 = 1$ and

$$\begin{aligned}
(\gamma u_{\varphi})^{p-1} &= \gamma^{p-1}u_{\varphi}^{p-1} = \zeta_{l^c}^{z(p-1)}\zeta_{2^{s+1}}^{p-1}\zeta_{l^c}^{-(p-1)/2}, \\
&= \zeta_{l^c}^{(2z-1)(p-1)/2}\zeta_{2^{s+1}}^{p-1} = \zeta_{2^{s+1}}^{p-1}.
\end{aligned}$$

In the above, note that $2z - 1 \equiv 0 \pmod{l^c}$. Write $p - 1 = 2^t \cdot y$, $(2, y) = 1$. As $p - 1$ divides $q - 1 = 2^s \cdot h'$, it follows that $t \leqslant s$ and $\zeta_{2^{s+1}}^{p-1}$ is a primitive 2^{s+1-t}-th root of unity. On the other hand, $U(k(\zeta_p)^{\mathfrak{p}}) = \langle \zeta_{q-1} \rangle$ and $N(k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, U(k(\zeta_p)^{\mathfrak{p}})) = \langle \zeta_{q-1}^{p-1} \rangle$. It is clear that the 2-Sylow subgroup of $\langle \zeta_{q-1}^{p-1} \rangle$ is $\langle \zeta_{2^{s-t}} \rangle$, and so $\zeta_{2^{s+1}}^{p-1} \notin N(k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, U(k(\zeta_p)^{\mathfrak{p}}))$. Hence we see that

$$[A(l^c, p)/\mathfrak{p}] = \tfrac{1}{2}, \qquad \text{if } l \neq 2 \text{ and } \mathfrak{p} \text{ is inertial in } Q(\zeta_{l^c}). \tag{22}$$

By the same argument as before, we have

$$B(l^c, p)_{\mathfrak{p}} \sim ((\gamma v_\varphi)^{p-1}, k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, \varphi),$$

$$(\gamma v_\varphi)^{p-1} = \gamma^{p-1} v_\varphi^{p-1} = -\zeta_{l^c}^{(2z-1)(p-1)/2} \zeta_{2^{s+1}}^{p-1} = -\zeta_{2^{s+1}}^{p-1}.$$

Consequently,

$$B(l^c, p)_{\mathfrak{p}} \sim A(l^c, p)_{\mathfrak{p}} \otimes_{k_{\mathfrak{p}}} (-1, k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, \varphi).$$

-1 belongs to $N(k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, U(k(\zeta_p)^{\mathfrak{p}})) = \langle \zeta_{q-1}^{p-1} \rangle$, if and only if $t < s$, i.e., if and only if $2(p-1)$ divides $p^{f/2} - 1$. Hence the cyclic algebra $(-1, k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, \varphi)$ has Hasse invariant zero at $\mathfrak{p}$, if and only if $2(p-1)$ divides $p^{f/2} - 1$. From this and (22), we conclude

$$\left(\frac{B(l^c, p)}{\mathfrak{p}}\right) = \begin{cases} 0, & \text{if } 2(p-1) \nmid p^{f/2} - 1, \\ \tfrac{1}{2}, & \text{if } 2(p-1) \mid p^{f/2} - 1, \end{cases}$$

provided that $l \neq 2$ and $\mathfrak{p}$ is inertial in $Q(\zeta_{l^c})$.

Suppose last that $l = 2$. Since we are assuming that $\mathfrak{p}$ is inertial in $Q(\zeta_{2^c})/k_{2,c}$, Lemma 4 implies that $p \equiv -1 \pmod{2^c}$. Write $p + 1 = 2^c h$. We fix a primitive $(p^2 - 1)$-th root of unity ζ_{p^2-1} such that $\zeta_{p^2-1}^{h(p-1)} = \zeta_{2^c}$. It is easily seen that $N(k_{\mathfrak{p}}/Q_p, \mathfrak{p}) = p$ and $U(K^{\mathfrak{p}}) = \langle \zeta_{p^2-1} \rangle$. Set $\gamma = \zeta_{p^2-1}^{(-1+2^{c-1})h}$. Then $\gamma^{p-1} = \zeta_{p^2-1}^{(-1+2^{c-1})h(p-1)} = \zeta_{2^c}^{-1+2^{c-1}} = -\zeta_{2^c}^{-1}$. Consequently, by (3), $u_\varphi u_\iota = -\zeta_{2^c}^{-1} u_\iota u_\varphi = \gamma^{p-1} u_\iota u_\varphi$, and so $(\gamma u_\varphi) u_\iota = \gamma^p u_\iota u_\varphi = u_\iota (\gamma u_\varphi)$. Here, we note that ι is the Frobenius automorphism of $K^{\mathfrak{p}}/k_{\mathfrak{p}}$. So, $\zeta_{p^2-1}^{\iota} = \zeta_{p^2-1}^{p}$, and $\gamma^\iota = \gamma^p$. Each element of $Q(\zeta_{2^c})^{\mathfrak{p}}$ (resp. $k(\zeta_p)^{\mathfrak{p}}$) commutes with γu_φ (resp. u_ι). Therefore we have

$$\begin{aligned} A(2^c, p)_{\mathfrak{p}} &\sim \sum_{\nu=0}^{p-1} \sum_{\mu=0}^{1} K^{\mathfrak{p}} (\gamma u_\varphi)^\nu u_\iota^\mu, \\ &= \left[\sum_\nu k(\zeta_p)^{\mathfrak{p}} (\gamma u_\varphi)^\nu\right] \cdot \left[\sum_\mu Q(\zeta_{2^c})^{\mathfrak{p}} u_\iota^\mu\right], \\ &\cong ((\gamma u_\varphi)^{p-1}, k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, \varphi) \otimes_{k_{\mathfrak{p}}} (1, Q(\zeta_{2^c})^{\mathfrak{p}}/k_{\mathfrak{p}}, \iota), \\ &\sim ((-1)^{h+1}, k(\zeta_p)^{\mathfrak{p}}/k_{\mathfrak{p}}, \varphi), \end{aligned}$$

where by (3),

$$(\gamma u_\varphi)^{p-1} = \gamma^{p-1}u_\varphi^{p-1} = -\zeta_{2^c}^{-1}\zeta_{2^c}^{-(p-1)/2} = -\zeta_{2^c}^{-1-(2^ch-2)/2},$$
$$= -\zeta_{2^c}^{-2^{c-1}h} = -(-1)^h = (-1)^{h+1}.$$

By the same argument, we have

$$B(2^c, p)_\mathfrak{p} \sim ((\gamma v_\varphi)^{p-1}, k(\zeta_p)^\mathfrak{p}/k_\mathfrak{p}, \varphi),$$
$$(\gamma v_\varphi)^{p-1} = \gamma^{p-1}v_\varphi^{p-1} = -\zeta_{2^c}^{-1}(-\zeta_{2^c}^{-(p-1)/2}) = (-1)^h.$$

Meanwhile, $U(k(\zeta_p)^\mathfrak{p}) = \langle\zeta_{p-1}\rangle$ and $N(k(\zeta_p)^\mathfrak{p}/k_\mathfrak{p}, U(k(\zeta_p)^\mathfrak{p})) = \langle\zeta_{p-1}^{p-1}\rangle = \langle 1\rangle$. Thus, we conclude that

$$[A(2^c, p)/\mathfrak{p}] = 0, \quad [B(2^c, p)/\mathfrak{p}] = \tfrac{1}{2}, \quad \text{if } p \equiv -1 \pmod{2^c}, \quad p \not\equiv -1 \pmod{2^{c+1}}, \tag{23}$$

and that

$$[A(2^c, p)/\mathfrak{p}] = \tfrac{1}{2}, \quad [B(2^c, p)/\mathfrak{p}] = 0, \quad \text{if } p \equiv -1 \pmod{2^{c+1}}. \tag{24}$$

4. Construction of Simple Algebras for $p = 2$

Throughout this section, l denotes an odd prime number. Set $K = Q(\zeta_{l^c}, \zeta_4)$ and $k = k_{l,c} = Q(\zeta_{l^c} + \zeta_{l^c}^{-1})$. Then, $K = Q(\zeta_{l^c}) \cdot k(\zeta_4)$ and $k = Q(\zeta_{l^c}) \cap k(\zeta_4)$. The Galois groups $\mathfrak{G}(K/k(\zeta_4))$ and $\mathfrak{G}(K/Q(\zeta_{l^c}))$ are cyclic of order 2 and generated by the automorphisms ι and φ respectively such that

$$\iota(\zeta_{l^c}) = \zeta_{l^c}^{-1}, \iota(\zeta_4) = \zeta_4, \varphi(\zeta_{l^c}) = \zeta_{l^c}, \varphi(\zeta_4) = \zeta_4^{-1}.$$

Then, $\mathfrak{G} = \mathfrak{G}(K/k) = \langle\iota\rangle \times \langle\varphi\rangle$. Define mappings α' and β' from $\mathfrak{G} \times \mathfrak{G}$ into $K^\times$ by the following formulas:

$$\alpha'(\iota^\nu\varphi^\mu, \iota^{\nu'}\varphi^{\mu'}) = (-\zeta_4)^{\nu'\gamma}\zeta_4^{\delta}, \tag{25}$$

$$\beta'(\iota^\nu\varphi^\mu, \iota^{\nu'}\varphi^{\mu'}) = (-\zeta_4)^{\nu'\gamma}\zeta_4^{\delta}(-1)^{\epsilon}, \tag{26}$$

$$(0 \leqslant \nu, \mu, \nu', \mu' \leqslant 1)$$

$$\delta = \begin{cases} 0, & \nu + \nu' < 2, \\ 1, & \nu + \nu' = 2, \end{cases} \quad \gamma = \begin{cases} 0, & \mu = 0, \\ 1, & \mu = 1, \end{cases} \quad \epsilon = \begin{cases} 0, & \mu + \mu' < 2, \\ 1, & \mu + \mu' = 2. \end{cases}$$

It is easily checked that α' and β' are factor sets of K/k (cf. Zassenhaus [12, III, §8]). Consider the following crossed products $C = C(l^c, 2)$ and

$D = D(l^e, 2)$ of K/k with its Galois group $\mathfrak{G}$, and having the factor sets α' and β' respectively:

$$C = (\alpha', K/k) = \sum_{\sigma\in\mathfrak{G}} Ku_\sigma \qquad \text{(direct sum)},$$
$$u_\sigma x = x^\sigma u_\sigma , \qquad u_\sigma u_\tau = \alpha'(\sigma, \tau)\, u_{\sigma\tau} \qquad (x \in K;\ \sigma, \tau \in \mathfrak{G}),$$
$$D = (\beta', K/k) = \sum_{\sigma\in\mathfrak{G}} Kv_\sigma \qquad \text{(direct sum)},$$
$$v_\sigma x = x^\sigma v_\sigma , \qquad v_\sigma v_\tau = \beta'(\sigma, \tau)\, v_{\sigma\tau} .$$

From the definition of α' and β', it follows easily that

$$u_\varphi u_\iota = -\zeta_4 u_\iota u_\varphi , \qquad u_\iota{}^2 = \zeta_4 , \qquad u_\varphi{}^2 = 1, \tag{27}$$
$$v_\varphi v_\iota = -\zeta_4 v_\iota v_\varphi , \qquad v_\iota{}^2 = \zeta_4 , \qquad v_\varphi{}^2 = -1. \tag{28}$$

The elements ζ_{l^e}, ζ_4, u_σ and u_ι generate a finite subgroup $G(l^e, 2)$ of the multiplicative group $C(l^e, 2)^\times$. In fact, $G(l^e, 2)$ is an extension of the normal cyclic subgroup $F_1 = \langle \zeta_{l^e}, \zeta_4 \rangle$ by an abelian group isomorphic to $\mathfrak{G}(Q(\zeta_{l^e}, \zeta_4)/k_{l,e})$, having the factor set α'. The crossed product $C(l^e, 2)$ is spanned by $G(l^e, 2)$ with rational coefficients, and so $C(l^e, 2)$ is isomorphic to a simple component of the group algebra $Q[C(l^e, 2)]$. Similarly, $H(l^e, 2) = \langle \zeta_{l^e}, \zeta_4, v_\varphi, v_\iota \rangle$ is a finite subgroup of $D(l^e, 2)^\times$. The crossed product $D(l^e, 2)$ is isomorphic to a simple component of $Q[H(l^e, 2)]$.

Now we proceed to calculate the Hasse invariants of $C(l^e, 2)$ and $D(l^e, 2)$. If $\mathfrak{q}$ is a prime ideal of $k_{l,e}$ which divide neither l nor 2, both $C(l^e, 2)$ and $D(l^e, 2)$ have Hasse invariant zero at $\mathfrak{q}$, because $\mathfrak{q}$ is not ramified in $Q(\zeta_{l^e}, \zeta_4)/k_{l,e}$ and the factor sets α' and β' consist of roots of unity. So, we have

$$[C(l^e, 2)/\mathfrak{q}] = [D(l^e, 2)/\mathfrak{q}] = 0, \qquad \text{for} \quad \mathfrak{q} \nmid l, 2. \tag{29}$$

From (27), it follows that

$$u_\varphi\{(1 - \zeta_4)\, u_\iota\} = (1 - \zeta_4^{-1})\, u_\varphi u_\iota = (1 - \zeta_4^{-1})(-\zeta_4)\, u_\iota u_\varphi = \{(1 - \zeta_4)\, u_\iota\}\, u_\varphi .$$

The elements $u_\varphi{}^\nu\{(1 - \zeta_4)\, u_\iota\}^\mu$ $(0 \leqslant \nu, \mu \leqslant 1)$ are linearly independent over K. Each element of $k(\zeta_4)$ (resp. $Q(\zeta_{l^e})$) commutes with $(1 - \zeta_4)\, u_\iota$ (resp. u_φ). Therefore, we have

$$\begin{aligned} C(l^e, 2) &= \sum_{\nu=0}^{1} \sum_{\mu=0}^{1} Q(\zeta_{l^e}, \zeta_4)\, u_{\varphi^\nu \iota^\mu} , \\ &= \sum_{\nu=0}^{1} \sum_{\mu=0}^{1} Q(\zeta_{l^e}) \cdot k(\zeta_4)\, u_\varphi{}^\nu\{(1 - \zeta_4)\, u_\iota\}^\mu , \\ &= \left[\sum_{\mu=0}^{1} Q(\zeta_{l^e})\{(1 - \zeta_4)\, u_\iota\}^\mu\right] \cdot \left[\sum_{\nu=0}^{1} k(\zeta_4)\, u_\varphi{}^\nu\right], \\ &\cong (\{(1 - \zeta_4)\, u_\iota\}^2, Q(\zeta_{l^e})/k, \iota) \otimes_k (u_\varphi{}^2, k(\zeta_4)/k, \varphi), \\ &\sim (2, Q(\zeta_{l^e})/k, \iota), \end{aligned} \tag{30}$$

where by (27), $\{(1-\zeta_4)u_\iota\}^2 = (1-\zeta_4)^2 u_\iota^2 = (1-\zeta_4)^2\zeta_4 = \zeta_4 - 2\zeta_4^2 + \zeta_4^3 = 2$, and $u_\omega^2 = 1$. By the same argument, we have

$$\begin{aligned} D(l^e, 2) &= \sum_{\nu=0}^{1}\sum_{\mu=0}^{1} Q(\zeta_{l^e}, \zeta_4)\, v_{\varphi^\nu \iota^\mu}, \\ &= \sum_{\nu=0}^{1}\sum_{\mu=0}^{1} Q(\zeta_{l^e}) \cdot k(\zeta_4)\, v_\varphi{}^\nu \{(1-\zeta_4)\, v_\iota\}^\mu, \\ &\cong (\{(1-\zeta_4)\, v_\iota\}^2, Q(\zeta_{l^e})/k, \iota) \otimes_k (v_\varphi{}^2, k(\zeta_4)/k, \varphi), \\ &= (2, Q(\zeta_{l^e})/k, \iota) \otimes_k (-1, k(\zeta_4)/k, \varphi), \\ &\sim C(l^e, 2) \otimes_k (-1, k(\zeta_4)/k, \varphi). \end{aligned} \tag{31}$$

Let $\mathfrak{p}$ be any prime ideal of $k = k_{l,e}$, which divides 2. Since k/Q is nonramified at 2, 2 is a prime element of the local field $k_\mathfrak{p}$. If $\mathfrak{p}$ is inertial in $Q(\zeta_{l^e})/k$, then the extension $Q(\zeta_{l^e})^\mathfrak{p}/k_\mathfrak{p}$ is nonramified of degree 2. By the definition of Hasse invariant and (30), $C(l^e, 2)$ has Hasse invariant $\frac{1}{2}$ at $\mathfrak{p}$. If $\mathfrak{p}$ splits into two primes, then $Q(\zeta_{l^e})^\mathfrak{p} = k_\mathfrak{p}$, and so $C(l^e, 2)$ has Hasse invariant zero. Since $\mathfrak{G}(Q(\zeta_{l^e})/Q)$ $(= Z \bmod^\times l^e)$ is cyclic and $\mathfrak{G}(Q(\zeta_{l^e})/k) = \langle -1 \bmod^\times l^e\rangle$, $\mathfrak{p}$ is inertial in $Q(\zeta_{l^e})/k$ if and only if $-1 \bmod^\times l^e \in \langle 2 \bmod^\times l^e\rangle$, i.e., if and only if the order of the cyclic group $\langle 2 \bmod^\times l^e\rangle$ is even. Consequently, we have

$$\left(\frac{C(l^e, 2)}{\mathfrak{p}}\right) = \begin{cases} 0, & \text{if } f \text{ is odd,} \\ \frac{1}{2}, & \text{if } f \text{ is even,} \end{cases} \quad (\mathfrak{p} \mid 2) \tag{32}$$

where f is the smallest positive integer such that

$$2^f \equiv 1 \pmod{l^e}. \tag{33}$$

The $\mathfrak{p}$-index of the cyclic algebra $(-1, k(\zeta_4)/k, \varphi)$ is equal to the order of the (local) norm residue symbol $(-1, k(\zeta_4)^\mathfrak{p}/k_\mathfrak{p})$, which is equal to the norm residue symbol $(N(k_\mathfrak{p}/Q_2, -1), k(\zeta_4)^\mathfrak{p}/Q_2)$. We see easily that the degree of $k_\mathfrak{p}$ over Q_2 is even if and only if $f \equiv 0 \pmod 4$. Hence,

$$N(k_\mathfrak{p}/Q_2, -1) = \begin{cases} 1, & \text{if } f \equiv 0 \pmod 4, \\ -1, & \text{otherwise.} \end{cases} \tag{34}$$

If there exists an element x of $k(\zeta_4)^\mathfrak{p}$ such that $-1 = N(k(\zeta_4)^\mathfrak{p}/Q_2, x) = N(Q_2(\zeta_4)/Q_2, N(k(\zeta_4)^\mathfrak{p}/Q_2(\zeta_4), x))$, then -1 belongs to the norm group $N(Q_2(\zeta_4)/Q_2, Q_2(\zeta_4)^\times)$. But this is impossible, because it is well-known that $-1 \notin N(Q_2(\zeta_4)/Q_2, Q_2(\zeta_4)^\times)$. (This follows from the fact that the quaternion algebra $(-1, Q(\zeta_4), \rho)$, $\rho(\zeta_4) = \zeta_4^{-1}$, has Hasse invariant $\frac{1}{2}$ at 2 and ∞.)

Consequently, the order of the norm residue symbol $(-1, k(\zeta_4)^{\mathfrak{p}}/Q_2)$ is equal to 2. Taking account of (34), we conclude that the Hasse invariant of the cyclic algebra $E = (-1, k(\zeta_4)/k, \varphi)$ at $\mathfrak{p}$ is

$$\left(\frac{E}{\mathfrak{p}}\right) = \begin{cases} 0, & \text{if } f \equiv 0 \pmod 4, \\ \frac{1}{2}, & \text{otherwise.} \end{cases} \tag{35}$$

Since by (31), $D(l^c, 2) \sim C(l^c, 2) \otimes_k E$, the formulas (32) and (35) imply that

$$\left(\frac{D(l^c, 2)}{\mathfrak{p}}\right) = \begin{cases} 0, & \text{if } f \equiv 0 \pmod 2 \quad \text{and} \quad f \not\equiv 0 \pmod 4, \\ \frac{1}{2}, & \text{if } f \text{ is odd or } f \equiv 0 \pmod 4. \end{cases} \tag{36}$$

Let $\mathfrak{p}_\infty$ be any infinite prime of $k_{l,c}$. From (30), it follows that

$$\begin{aligned} C(l^c, 2) \otimes_k k_{\mathfrak{p}_\infty} &\sim (2, Q(\zeta_{l^c})^{\mathfrak{p}_\infty}/k_{\mathfrak{p}_\infty}, \iota), \\ &\simeq (2, C/R, \rho)(\rho(\sqrt{-1}) = -\sqrt{-1}), \\ &\sim 1. \end{aligned}$$

We have

$$E \otimes_k k_{\mathfrak{p}_\infty} \sim (-1, k(\zeta_4)^{\mathfrak{p}_\infty}/k_{\mathfrak{p}_\infty}, \varphi) \simeq (-1, C/R, \rho).$$

Thus, we conclude that

$$[C(l^c, 2)/\mathfrak{p}_\infty] = 0 \qquad \text{and} \qquad [D(l^c, 2)/\mathfrak{p}_\infty] = \tfrac{1}{2}. \tag{37}$$

Let $\mathfrak{l}$ be the only prime ideal of $k = k_{l,c}$ which divides l. First we note that

$$(-1, k(\zeta_4)/k, \varphi) \otimes_k k_{\mathfrak{l}} \sim 1,$$

because the extension $k(\zeta_4)^{\mathfrak{l}}/k_{\mathfrak{l}}$ is nonramified of degree 2 or 1, and -1 is a unit. From (31), it follows that

$$D(l^c, 2) \otimes_k k_{\mathfrak{l}} \sim C(l^c, 2) \otimes_k k_{\mathfrak{l}},$$

and so,

$$[D(l^c, 2)/\mathfrak{l}] = [C(l^c, 2)/\mathfrak{l}]. \tag{38}$$

Suppose that $l \equiv 1 \pmod 4$. Then $\mathfrak{l}$ decomposes into two primes in $k(\zeta_4)/k$, and $\mathfrak{G}(K^{\mathfrak{l}}/k_{\mathfrak{l}}) = \mathfrak{G}(K/k(\zeta_4)) = \langle \iota \rangle$. Hence we have

$$\begin{aligned} C(l^c, 2) \otimes_k k_{\mathfrak{l}} &\sim \sum_{\mu=0}^{1} K^{\mathfrak{l}} u_\iota^{\mu} = (u_\iota^2, K^{\mathfrak{l}}/k_{\mathfrak{l}}, \iota), \\ &= (\zeta_4, K^{\mathfrak{l}}/k_{\mathfrak{l}}, \iota), \end{aligned}$$

where by (27), $u_\iota^2 = \zeta_4$. We see easily that $U(K^{\mathrm{I}}) = \langle \zeta_{l-1} \rangle$, where $U(K^{\mathrm{I}})$ is the set of roots of unity contained in K^{I}, whose orders are relatively prime to l. Then, $N(K^{\mathrm{I}}/k_{\mathrm{I}}, U(K^{\mathrm{I}})) = \langle \zeta_{l-1}^2 \rangle$, and ζ_{l-1}^2 is a primitive $(l-1)/2$-th root of unity. If $l \equiv 1 \pmod 8$, then $(l-1)/2 \equiv 0 \pmod 4$, and so $\zeta_4 \in \langle \zeta_{l-1}^2 \rangle$. If $l \equiv 5 \pmod 8$, then $(l-1)/2 \not\equiv 0 \pmod 4$, and so $\zeta_4 \notin \langle \zeta_{l-1}^2 \rangle$. Thus we conclude that

$$\left(\frac{C(l^c, 2)}{\mathrm{I}}\right) = \begin{cases} 0, & \text{if } l \equiv 1 \pmod 8, \\ \frac{1}{2}, & \text{if } l \equiv 5 \pmod 8. \end{cases} \tag{39}$$

Suppose next that $l \equiv 3 \pmod 4$. Then I is inertial in $k(\zeta_4)/k$, and $\mathfrak{G}(K^{\mathrm{I}}/k_{\mathrm{I}}) = \mathfrak{G}(K/k)$. We see that $U(K^{\mathrm{I}}) = \langle \zeta_{l^2-1} \rangle$ and φ is the Frobenius automorphism of $K^{\mathrm{I}}/k_{\mathrm{I}}$ such that $\zeta_{l^2-1}^{\varphi} = \zeta_{l^2-1}^{l}$. We note that $l^2 - 1 \equiv 0 \pmod 8$. So, all the primitive 8-th roots of unity are in $U(K^{\mathrm{I}})$. Since $l \equiv 3 \pmod 4$, $l - 1 \not\equiv 0 \pmod 4$. So we fix a primitive 8-th root of unity ζ_8 such that $\zeta_8^{l-1} = \zeta_4$. From (27), it follows that

$$\begin{aligned} u_\iota u_\varphi &= \zeta_4 u_\varphi u_\iota = \zeta_8^{l-1} u_\varphi u_\iota, \\ (\zeta_8 u_\iota) u_\varphi &= \zeta_8{}^{l} u_\varphi u_\iota = u_\varphi (\zeta_8 u_\iota). \end{aligned}$$

Each element of $k(\zeta_4)^{\mathrm{I}}$ (resp. $Q(\zeta_{l^c})^{\mathrm{I}}$) commutes with $\zeta_8 u_\iota$ (resp. u_φ). So, we have

$$\begin{aligned} C(l^c, 2) \otimes_k k_{\mathrm{I}} &\sim \sum_{\nu=0}^{1} \sum_{\mu=0}^{1} K^{\mathrm{I}} u_\varphi{}^{\nu} u_\iota{}^{\mu}, \\ &= \sum_{\nu} \sum_{\mu} k(\zeta_4)^{\mathrm{I}} \cdot Q(\zeta_{l^c})^{\mathrm{I}} u_\varphi{}^{\nu} (\zeta_8 u_\iota)^{\mu}, \\ &\cong ((\zeta_8 u_\iota)^2, Q(\zeta_{l^c})^{\mathrm{I}}/k_{\mathrm{I}}, \iota) \otimes_{k_{\mathrm{I}}} (u_\varphi{}^2, k(\zeta_4)^{\mathrm{I}}/k_{\mathrm{I}}, \varphi), \\ &\sim (\zeta_8{}^2 \zeta_4, Q(\zeta_{l^c})^{\mathrm{I}}/k_{\mathrm{I}}, \iota), \end{aligned} \tag{40}$$

where by (27), $(\zeta_8 u_\iota)^2 = \zeta_8{}^2 u_\iota{}^2 = \zeta_8{}^2 \zeta_4$ and $u_\varphi{}^2 = 1$. We write $l - 1 = 2(1 + 2s)$. If $l \equiv 3 \pmod 8$, then s is even. If $l \equiv 7 \pmod 8$, then s is odd. Since $\zeta_4 = \zeta_8^{l-1} = \zeta_8{}^2 \zeta_8^{4s} = (-1)^s \zeta_8{}^2$, it follows that if $l \equiv 3 \pmod 8$, then $\zeta_4 = \zeta_8{}^2$, and that if $l \equiv 7 \pmod 8$, then $\zeta_4 = -\zeta_8{}^2$. So, we have

$$\zeta_8{}^2 \zeta_4 = \begin{cases} -1, & \text{if } l \equiv 3 \pmod 8, \\ 1, & \text{if } l \equiv 7 \pmod 8. \end{cases} \tag{41}$$

We see that $U(Q(\zeta_{l^c})^{\mathrm{I}}) = \langle \zeta_{l-1} \rangle$ and $N(Q(\zeta_{l^c})^{\mathrm{I}}/k_{\mathrm{I}}, U(Q(\zeta_{l^c})^{\mathrm{I}})) = \langle \zeta_{l-1}^2 \rangle$. -1 does not belong to $\langle \zeta_{l-1}^2 \rangle$, because ζ_{l-1}^2 is a primitive $(l-1)/2$-th root of unity and $(l-1)/2$ is odd. So, the cyclic algebra $(-1, Q(\zeta_{l^c})^{\mathrm{I}}/k_{\mathrm{I}}, \iota)$ has Hasse invariant $\frac{1}{2}$ at I. From (40) and (41), it follows that

$$\left(\frac{C(l^c, 2)}{\mathrm{I}}\right) = \begin{cases} \frac{1}{2}, & \text{if } l \equiv 3 \pmod 8, \\ 0, & \text{if } l \equiv 7 \pmod 8. \end{cases} \tag{42}$$

Thus, by (38), (39) and (42), we have

$$\left(\frac{C(l^c, 2)}{\mathfrak{l}}\right) = \left(\frac{D(l^c, 2)}{\mathfrak{l}}\right) = \begin{cases} 0, & \text{if } l \equiv \pm 1 \pmod 8, \\ \frac{1}{2}, & \text{if } l \equiv \pm 5 \pmod 8. \end{cases} \tag{43}$$

5. Construction of Simple Algebras for $p = \infty$

Consider the following cyclic algebra $F(l^c, \infty)$ central over $k_{l,c}$:

$$\begin{aligned} F(l^c, \infty) &= (-1, Q(\zeta_{l^c})/k_{l,c}, \iota), \\ &= \sum_{i=0}^{1} Q(\zeta_{l^c})\, u_\iota^{\,i}, \qquad \text{(direct sum)} \\ u_\iota^{\,2} &= -1, \qquad u_\iota x = x^\iota u_\iota \qquad (x \in Q(\zeta_{l^c})), \end{aligned}$$

where ι is the automorphism of $Q(\zeta_{l^c})/k_{l,c}$ such that $\zeta_{l^c}^{\iota} = \zeta_{l^c}^{-1}$. If $l \neq 2$, then the elements ζ_{l^c}, -1, u_ι generate a finite subgroup G of the multiplicative group $F(l^c, \infty)^\times$. In fact, G is the metacyclic group with the following relations:

$$(-\zeta_{l^c})^{2l^c} = 1, \qquad u_\iota^{\,2} = -1, \qquad u_\iota(-\zeta_{l^c})\, u_\iota^{-1} = -\zeta_{l^c}^{-1} = (-\zeta_{l^c})^{-1}.$$

$F(l^c, \infty)$ is spanned by G with rational coefficients, and so it is isomorphic to a simple component of $Q[G]$. If $l = 2$, then $H = \langle \zeta_{2^c}, u_\iota \rangle$ is the generalized quaternion group of order 2^{c+1} and spans $F(2^c, \infty)$ with rational coefficients. So, $F(2^c, \infty)$ is isomorphic to a simple component of $Q[H]$.

For any infinite prime $\mathfrak{p}_\infty$ of $k = k_{l,c}$, we have

$$\begin{aligned} F(l^c, \infty) \otimes_k k_{\mathfrak{p}_\infty} &\sim (-1, Q(\zeta_{l^c})^{\mathfrak{p}_\infty}/k_{\mathfrak{p}_\infty}, \iota) \\ &\simeq (-1, C/R, \rho)(\rho(\sqrt{-1}) = -\sqrt{-1}). \end{aligned}$$

Therefore, we have

$$[F(l^c, \infty)/\mathfrak{p}_\infty] = \tfrac{1}{2}. \tag{44}$$

Let $\mathfrak{l}$ be the only prime ideal of $k = k_{l,c}$ which divides l. For simplicity, set $K = Q(\zeta_{l^c})$. The $\mathfrak{l}$-index of the cyclic algebra $F(l^c, \infty)$ is equal to the order of the (local) norm residue symbol

$$(-1, K^{\mathfrak{l}}/k_{\mathfrak{l}}) = (N(k_{\mathfrak{l}}/Q_l, -1), K^{\mathfrak{l}}/Q_l).$$

The extension k/Q is totally ramified at l, and so

$$[k_{\mathfrak{l}} : Q_l] = [k : Q] = \begin{cases} (l-1)\, l^{c-1}/2, & \text{if } l \neq 2, \\ 2^{c-2}, & \text{if } l = 2. \end{cases}$$

Since we have been assuming that $[k : Q] > 1$, it follows that

$$N(k_l/Q_l, -1) = \begin{cases} 1, & \text{if } l = 2 \text{ or } l \equiv 1 \pmod 4, \\ -1, & \text{if } l \equiv 3 \pmod 4. \end{cases}$$

Note that $U(K^l) = \langle \zeta_{l-1} \rangle$, and that $N(K^l/Q_l, U(K^l)) = \langle \zeta_{l-1}^{(l-1)l^{c-1}} \rangle = \langle 1 \rangle$, where $l \neq 2$. Hence if $l \equiv 3 \pmod 4$, then $N(k_l/Q_l, -1) = -1 \notin N(K^l/Q_l, U(K^l))$, and so the order of the norm residue symbol $(N(k_l/Q_l, -1), K^l/Q_l)$ is equal to 2. Thus we conclude that

$$\left(\frac{F(l^c, \infty)}{l}\right) = \begin{cases} 0, & \text{if } l = 2 \text{ or } l \equiv 1 \pmod 4, \\ \frac{1}{2}, & \text{if } l \equiv 3 \pmod 4. \end{cases} \tag{45}$$

For every finite prime $\mathfrak{q}$ of $k_{l,c}$ which does not divide l, we have

$$[F(l^c, \infty)/\mathfrak{q}] = 0, \tag{46}$$

because the extension $Q(\zeta_{l^c})/k_{l,c}$ is nonramified at $\mathfrak{q}$ and -1 is a unit.

6. Proof of the Theorem

We are ready to prove the Theorem. For each rational prime number l, we have constructed simple algebras $A(l^c, p)$, $B(l^c, p)$, $C(l^c, 2)$, $D(l^c, 2)$ and $F(l^c, \infty)$ which are central over $k_{l,c}$ and appear in some $Q[G]$. Recall that throughout this paper we are assuming $l^c \geqslant 5$. If A and B are central simple algebras over $k = k_{l,c}$ which appear in group algebras $Q[G]$ and $Q[H]$ respectively, then $A \otimes_k B$ appears in $Q[G \times H]$. For each rational prime p, g_p denotes the number of the primes of $k_{l,c}$ dividing p. We know that $g_l = 1$ and $g_\infty = [k_{l,c} : Q]$. If a central simple algebra A over $k_{l,c}$ satisfies the conditions (i) and (ii) of the Theorem, there exists a set of distinct rational primes $\{p_1, p_2, \ldots, p_n\}$ such that A has Hasse invariant $\frac{1}{2}$ at any prime $\mathfrak{p}$ of $k_{l,c}$ dividing one of $\{p_1, p_2, \ldots, p_n\}$ and zero elsewhere. By the Hasse's sum theorem, the number of those p_i for which g_{p_i} is odd is even. Conversely, let $\{p_1, p_2, \ldots, p_n\}$ be any set of distinct rational primes such that the number of those p_i for which g_{p_i} is odd is even. Again, by the Hasse's sum theorem, there exists a unique central division algebra $\Omega(p_1, p_2, \ldots, p_n)$ over $k_{l,c}$ which has Hasse invariant $\frac{1}{2}$ at any $\mathfrak{p}$ of $k_{l,c}$ dividing one of $\{p_1, p_2, \ldots, p_n\}$ and zero elsewhere. Of course, $\Omega(p_1, p_2, \ldots, p_n)$ satisfies the conditions (i) and (ii) of the Theorem.

Therefore, in order to prove the "if" part of the Theorem it suffices to show that for any p such that g_p is even, the central division algebra $\Omega(p)$

over $k_{l,c}$ belongs to $S_Q(k_{l,c})$, and that for any pair of distinct primes $\{p, p'\}$ such that both g_p and $g_{p'}$ are odd, $\Omega(p, p')$ belongs to $S_Q(k_{l,c})$. We shall do this for the cases $l = 2$, $l \equiv 1 \pmod 4$ and $l \equiv 3 \pmod 4$ separately.

(I) $l = 2$. Set $k = k_{2,c}$. Note that $[k_{2,c} : Q] = 2^{c-2} \geqq 2$. So g_p is odd if and only if $g_p = 1$, i.e., if and only if $p \equiv \pm 5 \pmod 8$ or $p = 2$. By virtue of (5), (7), (8), (9), (17), (18), (19), (23), (24), (44), (45), (46), and Lemma 4, we have the following results:

$$
\begin{aligned}
&A(2^c, p) \sim \Omega(p), \quad 2 \mid g_p, \quad \text{for} \quad p \equiv 1 \pmod 8,\ p \not\equiv 1 \pmod{2^{c+1}};\\
&B(2^c, p) \otimes_k F(2^c, \infty) \sim \Omega(p), \quad 2 \mid g_p, \ \text{for} \quad p \equiv 1 \pmod{2^{c+1}};\\
&A(2^c, p) \sim \Omega(2, p), \quad g_p = 1, \quad \text{for} \quad p \equiv 5 \pmod 8;\\
&B(2^c, p) \sim \Omega(2, p), \quad g_p = 1, \quad \text{for} \quad p \equiv -5 \pmod 8;\\
&B(2^c, p) \sim \Omega(p), \quad 2 \mid g_p, \quad \text{for} \quad p \equiv -1 \pmod 8,\ p \not\equiv -1 \pmod{2^{c+1}};\\
&A(2^c, p) \otimes_k F(2^c, \infty) \sim \Omega(p), \ 2 \mid g_p, \quad \text{for} \quad p \equiv -1 \pmod{2^{c+1}};\\
&F(2^c, \infty) \sim \Omega(\infty), \quad 2 \mid g_\infty, \quad \text{for} \quad p = \infty.
\end{aligned}
$$

From these formulas, it follows readily that for every p such that g_p is even, $\Omega(p) \in S_Q(k_{2,c})$, and that for every pair of distinct primes $\{p, p'\}$ such that $g_p = g_{p'} = 1$, $\Omega(p, p') \in S_Q(k_{2,c})$. For instande, if $p \equiv 5 \pmod 8$ and $p' \equiv -5 \pmod 8$, then $A(2^c, p) \otimes_k B(2^c, p') \sim \Omega(p, p')$, and so on. Thus, the "if" part of the Theorem is proved for $l = 2$.

Suppose that $l \neq 2$. For a rational prime number $p(\neq l)$, f_p denotes the smallest positive integer such that $p^{f_p} \equiv 1 \pmod{l^c}$, and set $g_p' = (l-1)\, l^{c-1}/f_p = \varphi(l^c)/f_p$. Then $g_p = g_p'$ or $2g_p = g_p'$. From Lemma 2, it follows easily that g_p' is even if and only if $(p/l) = 1$. We shall use the following well-known formulas:

$$
\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{[(l-1)/2][(p-1)/2]}, \qquad (l \neq p;\ l, p \neq 2), \tag{47}
$$

$$
\left(\frac{2}{l}\right) = (-1)^{(l^2-1)/8} = \begin{cases} 1, & \text{if} \quad l \equiv \pm 1 \pmod 8,\\ -1, & \text{if} \quad l \equiv \pm 5 \pmod 8. \end{cases} \tag{48}
$$

(II) $l \equiv 1 \pmod 4$. Since $g_\infty = [k_{l,c} : Q] = l^{c-1}(l-1)/2$, g_∞ is even. By (44), (45) and (46), we have

$$
F(l^c, \infty) \sim \Omega(\infty), \qquad 2 \mid g_\infty .
$$

Assume that $p \neq 2$. If f_p is odd, then $(p/l) = 1$ and 4 divides g_p', and so 2 divides g_p. If f_p is even, then by Lemma 3, any prime $\mathfrak{p}$ of $k = k_{l,c}$ dividing p is inertial in $Q(\zeta_{l^c})$. So, if f_p is even and $(p/l) = 1$, then $g_p = g_p'$, and this is even. If f_p is even and $(p/l) = -1$, then $g_p = g_p'$, and this is odd. From

(47), it follows that $(l/p) = (p/l)$. Therefore, by virtue of (5), (6), (8), (9), (16), (22), (44), (45) and (46), we have

$$B(l^c, p) \otimes_k F(l^c, \infty) \sim \Omega(p), \quad 2 \mid g_p \text{ for } 2 \nmid f_p,\ p \equiv 1 \pmod 4;$$
$$B(l^c, p) \sim \Omega(p), \quad 2 \mid g_p \text{ for } 2 \nmid f_p,\ p \equiv -1 \pmod 4;$$
$$A(l^c, p) \sim \Omega(p), \quad 2 \mid g_p \text{ for } 2 \mid f_p,\ (l/p) = 1,\ p \equiv 1 \pmod 4;$$
$$A(l^c, p) \otimes_k F(l^c, \infty) \sim \Omega(p), \quad 2 \mid g_p \text{ for } 2 \mid f_p,\ (l/p) = 1,\ p \equiv -1 \pmod 4;$$
$$A(l^c, p) \sim \Omega(l, p), \quad 2 \nmid g_p \text{ for } 2 \mid f_p,\ (l/p) = -1,\ p \equiv 1 \pmod 4;$$
$$A(l^c, p) \otimes_k F(l^c, \infty) \sim \Omega(l, p), \quad 2 \nmid g_p \text{ for } 2 \mid f_p,\ (l/p) = -1,\ p \equiv -1 \pmod 4.$$

Assume that $p = 2$. Suppose further that $l \equiv 1 \pmod 8$. By (48), g_2' is even. So, if f_2 is even, then $g_2 = g_2'$ and this is even. If f_2 is odd, then 4 divides g_2' and so 2 divides g_2. Suppose that $l \equiv 5 \pmod 8$. By (48), g_2' is odd, *a fortiori* g_2 is odd. From (29), (32), (36), (37) and (43), we conclude that

$$C(l^c, 2) \sim \Omega(2), \quad 2 \mid g_2 \quad \text{for} \quad l \equiv 1 \pmod 8, \quad 2 \mid f_2;$$
$$D(l^c, 2) \otimes_k F(l^c, \infty) \sim \Omega(2), \quad 2 \mid g_2 \quad \text{for} \quad l \equiv 1 \pmod 8, \quad 2 \nmid f_2;$$
$$C(l^c, 2) \sim \Omega(l, 2), \quad 2 \nmid g_2 \quad \text{for} \quad l \equiv 5 \pmod 8.$$

Thus, for any rational prime p, if g_p is even, then $\Omega(p) \in S_Q(k_{l,c})$, and if g_p is odd, then $\Omega(l, p) \in S_Q(k_{l,c})$. From these facts, the "if" part of the Theorem is easily proved for $l \equiv 1 \pmod 4$.

(III) $l \equiv 3 \pmod 4$. In this case, $[k_{l,c} : Q] = l^{c-1}(l-1)/2$, and this is odd. So, for every rational prime p, g_p is odd. By (44), (45) and (46), we have

$$F(l^c, \infty) \sim \Omega(l, \infty). \tag{49}$$

From Lemma 2, it follows readily that $(p/l) = 1$ if and only if g_p' is even, i.e., if and only if f_p is odd. By (47), if $(l/p) = 1$ and $p \equiv 1 \pmod 4$, then $(p/l) = 1$. Also, if $(l/p) = -1$ and $p \equiv 3 \pmod 4$, then $(p/l) = 1$. Otherwise $(p/l) = -1$ ($p \neq 2$). From (5), (6), (8), (9), (16) and (22), we have

$$B(l^c, p) \sim \Omega(p, \infty), \quad \text{for} \quad (l/p) = 1 \quad \text{and} \quad p \equiv 1 \pmod 4;$$
$$A(l^c, p) \sim \Omega(p, \infty), \quad \text{for} \quad (l/p) = 1 \quad \text{and} \quad p \equiv 3 \pmod 4;$$
$$A(l^c, p) \sim \Omega(l, p), \quad \text{for} \quad (l/p) = -1 \quad \text{and} \quad p \equiv 1 \pmod 4;$$
$$B(l^c, p) \sim \Omega(l, p), \quad \text{for} \quad (l/p) = -1 \quad \text{and} \quad p \equiv 3 \pmod 4.$$

If $l \equiv 3 \pmod 8$, it follows from (48) that f_2 is even. If $l \equiv 7 \pmod 8$, f_2 is odd. Hence, by (29), (32), (36), (37) and (43), we have

$$C(l^c, 2) \sim \Omega(l, 2), \quad \text{for} \quad l \equiv 3 \pmod 8;$$
$$D(l^c, 2) \sim \Omega(2, \infty), \quad \text{for} \quad l \equiv 7 \pmod 8.$$

Thus, we have shown that for every rational prime p ($\neq l, \infty$), either $\Omega(l, p) \in S_Q(k_{l,c})$ or $\Omega(p, \infty) \in S_Q(k_{l,c})$. By (49), we know that $\Omega(l, \infty) \in S_Q(k_{l,c})$. From these facts, we see easily that for any pair of rational primes $\{p, p'\}$ ($p \neq p'$), $\Omega(p, p')$ belongs to $S_Q(k_{l,c})$. For instance, if p ($\neq l, \infty$) is any prime such that $\Omega(p, \infty) \in S_Q(k_{l,c})$, then $\Omega(l, p) \sim \Omega(p, \infty) \otimes_k \Omega(l, \infty) \in S_Q(k_{l,c})$, where $k = k_{l,c}$. If p and p' are distinct primes such that $p, p' \neq l, \infty$, $\Omega(p, \infty) \in S_Q(k_{l,c})$, $\Omega(l, p') \in S_Q(k_{l,c})$, then

$$\Omega(p, p') \sim \Omega(p, \infty) \otimes_k \Omega(l, p') \otimes_k \Omega(l, \infty) \in S_Q(k_{l,c}),$$

etc. Thus the "if" part of the Theorem is proved for $l \equiv 3 \pmod 4$.

As for the "only if" part of the Theorem, the condition (i) follows from the Brauer–Speiser theorem, and the condition (ii) has been proved in [2]. The proof of the Theorem is completed.

Remark 1. Let $Q(\sqrt{m})$ be a real quadratic field such that m is square free and $m \equiv 3 \pmod 4$. Then, there exists a prime number l such that l divides m and $l \equiv 3 \pmod 4$. The extension $Q(\sqrt{m})/Q$ is ramified at l of degree 2. Let A be a simple algebra central over $k = Q(\sqrt{m})$ and $\mathfrak{l}$ the prime of k dividing l. If A appears in some $Q[G]$, $A \otimes_k k_{\mathfrak{l}}$ appears in $Q_l[G]$. Hence, by [11, Theorem 1], the $\mathfrak{l}$-index of A divides $(l - 1)/2$. Since $l \equiv 3 \pmod 4$, $(l - 1)/2$ is odd. On the other hand, the Brauer–Speiser theorem implies that the $\mathfrak{l}$-index of A divides 2. Consequently, the Hasse invariant of A at $\mathfrak{l}$ is equal to zero. Thus the statement of the Theorem does not hold for any real quadratic field $Q(\sqrt{m})$, $m \equiv 3 \pmod 4$.

Remark 2. Let k be a subfield of a cyclotomic extension of Q. In [2], the Schur subgroup $S(k)$ is defined as the subgroup of the Brauer group $\mathrm{Br}(k)$ consisting of those algebra classes which contain a simple component of $k[G]$ for some finite group G. Our Theorem implies that a class $\{A\}$ of $\mathrm{Br}(k_{l,c})$ belongs to $S(k_{l,c})$ if and only if $\{A\}$ has Hasse invariant zero or $\frac{1}{2}$ at every prime $\mathfrak{p}$ of $k_{l,c}$, and for any rational prime p, $\{A\}$ has the same Hasse invariant at all the primes $\mathfrak{p}$ of $k_{l,c}$ dividing p.

References

1. M. Benard, Quaternion constituents of group algebras, *Proc. Amer. Math. Soc.* **30** (1971), 217–219.
2. M. Benard, The Schur subgroup I, to appear.
3. M. Benard and M. M. Schacher, The Schur subgroup II, to appear.
4. M. Deuring, "Algebren," 2nd edition, Springer, Berlin, 1968.
5. K. L. Fields, On the Brauer–Speiser theorem, *Bull. Amer. Math. Soc.* **77** (1971), 223.
6. K. L. Fields and I. N. Herstein, On the Schur subgroup of the Brauer group, *J. Algebra* **20** (1972), 70–71.

7. H. HASSE, "Vorlesungen über Zahlentheorie," Springer, Berlin, 1950.
8. J.-P. SERRE, "Corps locaux," 2nd edition, Hermann, Paris, 1968.
9. B. L. VAN DER WAERDEN, "Algebra, II," 3rd edition, Springer, Berlin, 1955.
10. T. YAMADA, On the group algebras of metabelian groups over algebraic number fields II, *J. Fac. Sci. Univ. Tokyo* **16** (1969), 83–90.
11. T. YAMADA, Characterization of the simple components of the group algebras over the p-adic number field, *J. Math. Soc. Japan* **23** (1971), 295–310.
12. H. J. ZASSENHAUS, "The Theory of Groups," 2nd edition, Chelsea, New York, 1958.